

REMARKS

Entry of the amendments to the specification, claims and abstract before examination of the application is respectfully requested. These claims patentably define over the art of record.

If there are any questions regarding this Preliminary Amendment or the application in general, a telephone call to the undersigned would be appreciated since this should expedite the prosecution of the application for all concerned.

If necessary to effect a timely response, this paper should be considered as a petition for an Extension of Time sufficient to effect a timely response, and please charge any deficiency in fees or credit any overpayments to Deposit Account No. 05-1323 (Docket # 095309.56901US).

Respectfully submitted,



Gary R. Edwards
Registration No. 31,824

CROWELL & MORING LLP
Intellectual Property Group
P.O. Box 14300
Washington, DC 20044-4300
Telephone No.: (202) 624-2500
Facsimile No.: (202) 628-8844
GRE:kms
2652324v1

METHOD FOR SAFEGUARDING THE INTEGRITY AND AUTHENTICITY OF
FLASHWARE FOR CONTROL UNITS

BACKGROUND AND SUMMARY OF THE INVENTION

[0001] This application claims the priority of German patent document 103 18 031.1, filed April 19, 2003 (PCT International Application No. PCT/EP2004/002194, filed March 4, 2004), the disclosure of which is expressly incorporated by reference herein.

[0002] The invention relates to a security concept system for the software downloading software into process in a control unit.

[0003] The increasing presence of electronics in motor vehicles, and together with the increasing possibilities for communicating in a vehicle and with a vehicle, have [[also]] entailed [[an]] a corresponding increase in the demands made of upon security. Nowadays, microcontrollers are used for control purposes in various areas of technology, and ~~These control units are nowadays often~~ frequently connected to one another via a bus system ~~and there are usually possibilities of accessing this bus from the outside and that is externally accessible for~~ communicating with the individual control units. The ~~method of functioning~~ functionality of the control units is determined [[here]] by application programs, which, ~~These application programs have~~ in the past, have usually been stored in a nonprogrammable memory, preferably in the control unit. As a result, the software cannot be readily tampered with. For example, the complete

replacement of a memory module with another memory module can be detected and ~~correspondingly reacted to~~ dealt with.

[0004] ~~[[The]]~~ However, the future use of programmable control units, in particular what are referred to as flash-programmable control units, in vehicles ~~[[makes]]~~ increases the risk of ~~however greater that~~ unauthorized manipulations ~~will be carried out~~ to the application programs and thus to the ~~method of~~ operation of the control units. For this reason it is necessary to take measures which prevent unauthorized overwriting of application programs in the control units.

[0005] A typical downloading process for an application program, referred to as flashware, is disclosed ~~by the~~ in German patent document DE 195 06 957 C2. In this system, such an application program, ~~referred to as flashware,~~ is stored in a nonvolatile electrically erasable and programmable memory~~[[,]]~~ (referred to in the specialist field as a flash EPROM memory, or for short as a “flash”). ~~For this purpose, an~~ An initialization routine ~~[[is]]~~ stored in the boot area in the flash ~~electrically erasable and programmable read write memory (flash). This initialization routine~~ is used to load and start the user programs when the microprocessor system is put into operation.

[0006] In order to be able to replace an existing application program with a new one, the initialization routine additionally contains what is referred to as a reloading routine, which ~~This reloading routine~~ is activated by ~~means of~~ a special instruction via a system interface. After activation, the reloading routine ~~firstly~~ first stores the new application program in a buffer. A cyclic block

protection method is used to check whether ~~[[or not]]~~ the storing of the new application program was faulty. If ~~it the new application program~~ was transmitted and buffered correctly, the erasure of the user program which is to be replaced is initiated and carried out. For this purpose, the new application program is overwritten over the old application program in the erasable and programmable read-write memory (flash).

[0007] This process of programming and copying into the flash can also be checked by means of a cyclic block protection method, which however, ~~Checking by means of a cyclic block protection method only~~ makes it possible only to check ~~to what~~ the extent to which the program has been copied correctly. Checking for data integrity and authenticity is not possible with cyclic block protection methods. An unauthorized program or unauthorized flashware cannot be detected with cyclic block protection methods.

[0008] On the other hand, encryption methods and digital signature methods are known from the field of the Internet, in particular for home banking and home-shopping applications. The basis ~~[[of]]~~ for all the encryption methods ~~[[which]]~~ that are widespread today is what is referred to as public key encryption. ~~[[These]]~~ Such encryption algorithms operate with a secret key and ~~[[with]]~~ a public key; ~~[[, and]]~~ the ~~public key~~ latter may be known publicly, while the secret key may be known only to an authorized party, for example a trust center. Such cryptographic algorithms are, for example, Rivest, Shamir and Adelman (RSA algorithm) data encryption algorithm (DEA algorithm) or the like. With the secret or public key it is possible, in a fashion which is analogous

to a handwritten signature, to produce a digital signature for an electronic document. Only the user of the secret or public key can produce a valid signature. The genuineness of the document can then be checked by verifying the signature using the associated public or secret key. The secret key is sometimes also referred to as a private key.

[0009] The electronic signature has become known as a signature method. The purpose of the electronic signature is to ensure that a message reliably comes from a certain sender, and that it ~~this message~~ has not been falsified during the transmission.

[0010] Once the sender has generated a public key and a private key, the following method is conceivable:

[0011] The sender of the information uses his own private key to encrypt a message which can be read with the public key of the sender. A message which can be read with the public key can only originate from the sender because only the sender has the matching private key. The system is such that the private key can be used only for encryption while the public key can be used only for decryption or reading. Therefore, messages are produced which can be written by only one person, but can be read by all persons having the public key.

[0012] The encryption of the entire message ~~is relatively computing time intensive with~~ using the abovementioned encryption methods is relatively intensive in terms of computing time, and it is ~~not necessary~~ unnecessary for the

purpose of defining only the authenticity of the author. For this reason, a somewhat different method is used in practice:

- The sender calculates a type of summary or checksum of the message, referred to as the hash code. The calculation rule here is such that it is virtually impossible to change the message without simultaneously changing the hash code.

- The sender then encrypts the hash code with his private key. This is the electronic signature. The signature is therefore different for each message, only the length of the signature is always the same, irrespective of the length of the message. ~~This is the (a property of the hash codes), which always have the same length.~~

- The message is then sent with the signature.

- The receiver decrypts the signature with the public key of the sender and then receives the hash code acquired from the sender.

- The receiver himself can then determine the hash code of the original message and compare it with the hash code which has also been sent by the sender. If both hash codes correspond, it is ensured that the message actually originates from the one sender and that it has not been falsified on the transmission path.

[0013] The abovementioned signature method for [[the]] deciphering is based on the public key method RSA, and for the calculation of the hash code on the hash function RIPEMD-160.

[0014] Finally, by combining encryption and an electronic signature it is possible to send messages which can be reliably and unambiguously assigned to a sender before falsification.

[0015] [[A]] German patent document DE 100 08 974 A1 discloses a signature method for ensuring the data integrity of software for a control unit in a motor vehicle ~~has been proposed on the basis of~~ based on the abovementioned encryption ~~method~~ and signature method ~~in German patent application DE 100 08 974 A1~~. In this method, the public key is stored in a memory area of the control unit, and the [[. The]] software which is to be fed in[[,]] (referred to as the flashware) [[,]] is signed with a second secret key. In order to feed in the signed software, this flashware is ~~firstly~~ first stored in a memory on the control unit. The signature of the flashware is checked with the public key stored in the control unit itself. If the checking of the electronic signature has a positive result, the buffered flashware is read into an electronically erasable and programmable memory on the control unit, referred to as the flash.

[0016] Not all control units are capable of calculating the public key algorithms since some of them cannot support sliding decimal point arithmetic or make available sufficient memory space. In order to be able to form RSAs reliably, at present at least 1024 byte should be selected as the key length. It is

therefore impossible to use the abovementioned signature methods in many of the control units which are currently used in motor vehicles.

[0017] Taking the abovementioned prior art as a point of departure, ~~[[an]]~~ one object ~~according to~~ of the invention is to provide ~~specify~~ a simplified signature method which can be used on as ~~[[far]]~~ nearly as possible all control units in contemporary motor vehicles.

~~This object is achieved according to the invention by means of a method having the features of the independent claims. Further advantageous refinements of the invention are contained in the subclaims and in the description of the exemplary embodiments.~~

[0018] This and other objects and advantages are achieved by the ~~object is achieved by means of a~~ simplified symmetrical, cryptographic method~~[[.]]~~ according to the invention, which is based on ~~The basis of this method is an~~ authentication code that ~~. This authentication code~~ is calculated in a secured area~~[[,]]~~ (referred to as a trust center) ~~[[,]]~~ by concatenating the application program, (referred to as the flashware) ~~[[,]]~~ with a secret data string and calculating a hash value from the concatenated application program. ~~[[This]]~~ The hash value, which is calculated ~~here by means of~~ by the application program and ~~by means of using~~ the secret data string, ~~. This hash value~~ is the authentication code for the application program to be checked.

[0019] The authentication code is checked in the microprocessor system or in the control unit in which the application program is to be used. For this purpose,

a second, identical, secret data string is stored in the microprocessor system or the control unit. ~~Firstly,~~ First, the unencrypted application program and the authentication code are transmitted into the microprocessor system or into the control unit. The unencrypted application program is then concatenated with the second, identical, secret data string in the microprocessor system or in the control unit. A hash value is calculated by this concatenated application program in the microprocessor system or in the control unit. If the calculated hash value and the transmitted authentication code correspond, the transmitted application program or the transmitted firmware is considered to be authentic and is allowed to be stored in the flash memory and applied in the control unit or in the microprocessor system.

[0020] In ~~a development~~ one embodiment of the invention, the application program is concatenated with the secret data string at both ends, both at the start of the program and at the end of the program. The hash value is then calculated by means of the application program which is concatenated at both ends. In order to check the authentication code which is formed in this way, in the microprocessor system or in the control unit the application program which is transmitted in unencrypted form is also concatenated at both ends with the second, secret data string stored in the control unit, and a hash value is formed in the control unit or in the microprocessor system by means of the application program which is concatenated at both ends. If the hash value calculated in the control unit or in the microprocessor system corresponds to the transmitted authentication code, the transmitted application program is considered to be

authentic. The concatenation at both ends has the advantage of improved protection against unacceptable manipulations of the application software.

[0021] A further improvement with respect to manipulations is obtained by calculating a hash value twice. In this embodiment of the invention, the application program is ~~firstly~~ first concatenated at one end with a secret data string, and a hash value is then calculated by the application program which is concatenated at one end. The concatenation can be at the start of the program or at the end of the program here. This first hash value HMAC1 is in turn concatenated with this secret data string at one end. The concatenation may be carried out here at each end of the first hash value. Finally, in order to calculate an authentication code a second hash value HMAC is then calculated ~~by means of using~~ the combination of the data string and first hash value HMAC1, in a further ~~following~~ step.

[0022] In order to check the authentication code in the control unit or in the microprocessor system, the abovementioned calculation steps must be repeated in the same sequence in the microprocessor system or in the control unit. If the calculated hash value corresponds to the transmitted authentication code, the transmitted application software is therefore considered to be error free.

[0023] For the process of downloading the flashware itself there are various transmission possibilities. The flashware and authentication code may be transmitted together on the same distribution channel; or alternatively the authentication code may be transmitted on separate distribution channels by means of the application program. With separate transmission it is

advantageous to market the flashware or the application program on hardware storage media. Compact discs, EPROMs or memory cards are possible as preferred storage media.

[0024] When the application program which is to be transmitted into the flash memory of the system is successfully authenticated, ~~the new application program~~ it is preferably provided with an identifier, referred to as a flag, which. ~~This identifier identifies it as the application program as the respectively valid application program.~~

[0025] The invention mainly achieves the following advantages:

[0026] Not all control units are capable of calculating the public key algorithms since some of them cannot support sliding decimal point arithmetic, or cannot [[or]] make available sufficient memory space ~~to be able~~ to carry out the necessary encryption calculations. In order ~~to be able~~ to form the public key algorithms reliably, at present at least 1024 byte should be selected as the key length. Since many control units in motor vehicles only have a memory area of only 4 kbyte, the key alone would ~~already~~ take up a large part of the memory.

[0027] The invention also does not require encryption algorithms. [[here.]] The single calculation method which is used is to calculate hash values. By using the symmetrical, cryptographic method according to the invention it is also possible to equip these control units with an authentication check for which public key methods cannot be applied.

[0028] The method according to the invention is what is referred to as a message authentication code method which is based on the calculation of a hash value. There is therefore no signature method, such as. ~~A signature method~~ requires the receiver of a message to be incapable of copying the signature which is also supplied. For application in embedded systems ~~[[,]]~~ (for example, control units), a signature method is not necessary since the receiving control unit does not automatically form the message authentication code for a message. The control unit merely checks a given, secret data string for a given message. It is necessary to calculate a hash value in order to secure the transmission path. According to the invention, only the hash value of a message authentication code is in fact transmitted, and not the secret data string. The proposed hash value method according to the invention is significantly more efficient in terms of running time and memory space than enciphering and deciphering methods such as, for example, the public key algorithms, can be.

[0029] ~~Flashware meta information can also be included in the authentication code. Flashware meta information is,~~ (for example, the storage location of a flashware, the identification number of the flashware, the identification number of the control unit or the vehicle identification number) can also be included in the authentication code. Since this ~~[[. This]]~~ flashware meta information is integrated into the secret data string, the ~~[[. The]]~~ formation of a hash value by means of the flashware and ~~by means of~~ the secret data string thus ensures that the flashware meta information is also protected against manipulations on the transmission path.

[0030] If the same flashware is used on a plurality of control units, including the flashware meta information in the authentication code makes it possible to select the downloading process for flashware into the various control units using this authentication code. Since various control units have various identification numbers, and the storage locations for the flashware in the various control units are different, even when the flashware is the same there is a control unit-specific authentication code in each case according to the inventive method.

[0031] Other objects, advantages and novel features of the present invention will become apparent from the following detailed description of the invention when considered in conjunction with the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

~~Exemplary embodiments of the invention are explained below in more detail with reference to the figures. In the drawing:~~

[0032] Fig. 1 is a schematic diagram of a process for downloading flashware from a data memory to the control unit of a motor vehicle;

[0033] Fig. 2 is a schematic diagram of a process for downloading flashware in which the flashware and the authentication code enter the control unit of a motor vehicle on separate distribution channels;

[0034] Fig. 3 is a flowchart showing the calculation of an authentication code for the downloading process according to fig. 1;

[0035] Fig. 4 is a more ~~complicated~~ detailed flowchart showing the calculation of an authentication code for the downloading process according to fig. 1;

[0036] Fig. 5 is a flowchart showing the calculation of an authentication code for the downloading process according to fig. 2;

[0037] Fig. 6 is a more ~~complicated~~ detailed flowchart showing the calculation of an authentication code for the downloading process according to fig. 2; and

[0038] Fig. 7 is a block diagram of a microprocessor system or of a control unit having a flash memory into which an application program can be downloaded with the method according to the invention.

DETAILED DESCRIPTION OF THE DRAWINGS

[0039] Figure 1 shows a possible downloading process in which the invention is used. After the program development has been concluded, the application programs and/or the flashware are collected in a data memory 1. The individual application programs or application RAM packets 2 are transferred on a secured path to what is referred to as a trust center 3, where they ~~The application programs~~ are identified with an authentication code ~~in the trust center itself~~. (The sequences in the trust center itself are explained in more detail below in conjunction with figures 3 to 6.) The unencrypted flashware, together with the authentication code HMAC is transferred from the trust center to an external system interface 4, which ~~The system interface itself can be composed in the simplest case, may be~~ ~~[[of]]~~ a diagnostic connection in the motor vehicle.

(However, the system interface is generally formed by the diagnostic system in motor vehicle workshops.)

[0040] For transmitting from the trust center to the system interface it is possible ~~[[here]]~~ to use the customary data communication paths; ~~[[,]]~~ that is, ~~to say~~ in particular fixed network connections, Internet connections and also mobile radio connections. The system interface brings about the process of downloading the transmitted program package or the transmitted flashware and the authentication code HMAC into a control unit of a motor vehicle. For this purpose, ~~it the system interface~~ transmits to the control unit in the motor vehicle a special command, with which the flashware memory in the motor vehicle is prepared for the downloading process, ~~to the control unit in the motor vehicle~~. (The programming of the new application program into the flash memory is explained in more detail below in conjunction with figure 7.)

[0041] The transmitted authentication code HMAC is checked in the control unit of the motor vehicle and when successful checking occurs the flashware which is also transmitted is programmed into the flash memory of the control unit. The checking of the authentication code in the control unit of the motor vehicle is essentially carried out by repeating the steps with which the authentication code in the trust center was generated. (More details on the checking of the authentication code can be found below in the figure descriptions relating to figures 3 to 6.)

[0042] Figure 2 shows another ~~possibility for a~~ embodiment of the downloading process according to the invention, in which ~~In this exemplary~~

~~embodiment also, the application programs (“flashware”) are also~~ ~~[[are]]~~ collected in a data memory 1, ~~and . The application programs, referred to as the flashware, are~~ then transferred as program packages 2 to a trust center. An authentication code is generated for the flashware in the trust center 3, ~~using a~~ ~~[[. The]]~~ calculation ~~that is of the authentication code will be~~ explained in more detail ~~[[below]]~~ in conjunction with figures 5 and 6.) In contrast to the downloading process according to figure 1, with the downloading process described here only an authentication code HMAC is transmitted from the trust center to the system interface 4. The application program itself~~[[,]]~~ (the so-called flashware) ~~[[,]]~~ is transferred on a separate distribution channel.

[0043] The flashware is preferably recorded on compact discs, storage cards, EPROMs or other hardware storage means 6 and transmitted into the control unit 5 of the motor vehicle using a suitable reading device 7. In particular in the case of compact discs, the suitable reading device 7 in the motor vehicle may be ~~formed by~~ an infotainment system such as is used today in motor vehicles, ~~in particular by~~ (for example, a CD-ROM disk drive or a DVD disk drive).

[0044] In the exemplary embodiment according to figure 2 the downloading process is also initiated in the vehicle by means of a special command from the system interface 4, which for ~~[[. For]]~~ this purpose, ~~the system interface 4~~ has access to the data buses of the onboard power system in the motor vehicle. The reading in of the flashware from the reading device 7 into the control unit 5 is started by the system interface using a software command. At the same time, the

software command is used to prepare the flash memory of the control unit 5 for the transfer of the flashware.

[0045] The checking of the authentication code HMAC in a control unit will be explained in more detail below in the figure descriptions relating to figures 5 and 6. In principle, in order to check the authentication code, the calculation steps which were necessary to produce the authentication code ~~have to~~ must be repeated in the control unit in the same order as in the trust center.

[0046] In this exemplary embodiment, the system interface can also be formed in the simplest case by diagnostic connection in the motor vehicle. However, the system interface is preferably the diagnostic system in the motor vehicle workshop. Moreover, the ~~[[The]]~~ previously described checking of the authentication code applies irrespective of the selection of the transmission path for the flashware. The authentication sequence is the same when downloading the flashware from CD-ROM or DVD as when directly downloading the flashware from the central system by means of wirefree or wirebound data transmission.

[0047] All the exemplary embodiments of the invention have in common the calculation of a hash value. The hash function, known by the designation RIPEMD-160 algorithm, can be used to generate a check value, also called copy, of fixed length for data of any desired length. This copy is referred to as a hash value. A hash function and a hash value ~~fulfil~~ have the following properties:
[[here:]]

- The hash value is easy to calculate.
- It is virtually impossible to generate, for a given hash value, a data record which supplies this hash value (oneway function). In addition it is difficult to find a collision, *i.e.*, two data records with the same hash value (collision resistance).
- The hash function can be applied only for data or data records whose bit length is $2^{64} - 1$ at maximum. In the case of relatively short data records, the data records are filled with zeros until the length of the filled-in data record has an integral multiple of 512 bit. The filled-in data record is then divided into at least 512 bit long blocks. Applying the hash function to the 512 bit long blocks finally results in a 160 bit long hash value. The function can be applied here to any desired data records, in particular also to flashware.

[0048] Figure 3 shows a flowchart for calculating an authentication code within a secured area 3, referred to below as a trust center. In the trust center, secret identifiers in the form of data strings are managed in digital form in a separate, secured area, preferably a separate, secured data memory 8. The flashware for which an authentication code is to be calculated is firstly concatenated with a data string at both ends of the application program. That is, ~~to say~~ a secret data string from the memory 8 of the trust center is appended to the digital data record of the application program at the start and at the end. In the next step, a hash value is calculated for the flashware which is concatenated at both ends. This hash value contains all the information about the flashware and about the secret data string. Due to the previously explained properties of

the hash function, this hash value is suitable as an authentication code HMAC for the authenticity and the data integrity of the flashware. In the next step, the authentication code HMAC is added to the unencrypted application program, the so-called flashware, and transferred from the trust center to the system interface for further transmission into the motor vehicle.

[0049] Figure 4 shows a more complicated sequence for calculating an authentication code in a trust center. In this ~~exemplary~~ embodiment, the flashware is ~~firstly~~ first concatenated at one end with a secret data string. ~~The concatenation can take place either at the start or [[else]] at the end of the data record of the flashware. A first hash value calculation can be carried out by means of using the flashware which is concatenated at one end, generating a [[. A]] first hash value HMAC1 is obtained. This first hash value HMAC1 is in turn, concatenated at one end with a secret data string from the memory 8, once again. Here too, the concatenation can be carried out at the start or at the end of the first hash value. In a further step, a second hash value calculation is carried out by means of the combination of the secret data string and first hash value. The result of this last hash value calculation provides the authentication code HMAC. Unencrypted original flashware is then added to the authentication code and transmitted to the system interface. The exemplary embodiment in figure 4 is suitable for a downloading process according to figure 1.~~

[0050] Figure 5 ~~[[shows]]~~ is a flowchart showing the calculation of an authentication code within a trust center for use in the downloading process according to figure 2. In the trust center, the unencrypted original flashware is

concatenated at both ends with a secret data strength. In the next step, a hash value calculation is carried out for the flashware which is concatenated at both ends, thereby generating. ~~The result of this hash value calculation is the~~ authentication code HMAC.

[0051] In contrast to the exemplary embodiment in figure 3, in the exemplary embodiment in figure 5 only the authentication code is transmitted to the system interface. The marketing of the original and unencrypted flashware is carried out here on separate distribution channels. The flashware is preferably transferred here to hardware storage elements and read into the motor vehicle (see figure 2 for more details on this).

[0052] Figure 6 shows a further ~~exemplary~~ embodiment of a more complex calculation of an authentication code such as is used in conjunction with downloading processes according to figure 2. In this ~~exemplary~~ embodiment, the unencrypted flashware is ~~firstly~~ first concatenated at one end with a secret data string in the trust center, ~~The concatenation can be carried out here either at the start or at the end of the data record of the flashware. A hash value calculation is carried out by means of the flashware which is concatenated at one end, generating~~. ~~The result is~~ a first hash value HMAC1. This first hash value HMAC1 is in turn concatenated at one end with a secret data string from the memory 8. Here too, the concatenation can be carried out at the start or at the end of the first hash value. In a further step, a second hash value calculation is carried out by means of the combination of a secret data string and first hash value. The result of this last hash value calculation provides the authentication

code HMAC, which ~~This authentication code~~ is transferred to the system interface. In contrast to the exemplary embodiment in figure 4, in the exemplary embodiment in figure 6 only the authentication code is transferred to the system interface. Here, analogous to figure 2, the unencrypted original software is read into the motor vehicle by means of storage media, preferably compact discs.

[0053] More details will be given below on the flash process in the control unit or in the microprocessor system of the motor vehicle with reference to figure 7. A typical control unit, also referred to as electronic control unit ECU, contains a computing unit ~~, referred to as (a microprocessor CPU)~~, which is connected via a processor bus PBUS to various memories or memory sectors. Via an interface, the control unit can either be addressed from the outside or can communicate with other units connected to the interface. The memory of the control unit is composed of a boot sector, a flash memory, and a main memory RAM. The flash memory Flash is an electrically erasable and programmable memory, for example an EEPROM. The operating system of the microprocessor, referred to as a flash boot loader, and the RIPEMD-160 algorithm for the hash function are stored in the boot sector.

[0054] A secret data string is stored in the control unit in a memory or memory area 9 which is specially protected against external access, and may ~~This special protected data area 9 can also~~ be arranged in the boot area, or provided ~~Another possibility is to embody this specially protected data memory~~ 9 in the form of a memory card which cannot be overwritten and is protected against unauthorized reading out, or in the form of what is referred to as a

cryptoprocessor which erases its contents when unauthorized access is attempted. These measures and the embodiment of the specially protected memory area 9 ensure that the data string stored therein is kept secret. Which data strings are programmed in the specially protected data area 9 must be coordinated with the data strings for calculating the authentication codes in the trust center. The data string in the control unit must correspond to the data string which was used as the basis for calculating the authentication code.

[0055] The application programs which can be used as flashware are stored in the flash of the control unit. User programs which have already been stored are overwritten with new flashware basically in the following way. The control unit is prepared for a downloading process and for a flash process by ~~means of~~ a special software command which is transmitted from an external system interface via the interface of the control unit. What is referred to as the flash boot loader is actuated by means of the software command. The flash boot loader is essentially a reloading routine with which application programs are written into the flash memory of the control unit. During the downloading process, the new flashware and the transmitted authentication code are ~~firstly~~ first buffered in the main memory of the control unit. The ~~checking of the~~ buffered flashware and ~~[[of]]~~ the buffered authentication code are then checked for authenticity and data integrity ~~is then carried out~~ in the microprocessor of the control unit, using the reloading routine of the flash boot loader. This checking is carried out in such a way that the same method steps which were applied to generate the transmitted authentication code are carried out in the microprocessor with the

unencrypted software and the secret data string which is stored in the control unit. Those method steps which are carried out in the trust center in order to generate the authentication code are therefore repeated in the microprocessor of the control unit. If, for example, the authentication code was generated according to the exemplary embodiment in figure 3, in the microprocessor of the control unit the buffered flashware is concatenated at both ends with the secret data string stored in the control unit. The flashware which is concatenated at both ends carries out a hash value calculation using the RIPEMD-160 algorithm. The result of this hash value calculation in the control unit is compared with the transmitted identification code HMAC. If both hash values are identical, the flashware buffered in the main memory is considered to be authentic and integral. If the authentication code in the trust center was acquired according to one of the exemplary embodiments corresponding to figures 3, 4, 5 or 6, the concatenations of the buffered flashware with the secret data string stored in the control unit and the hash value calculations of the concatenated flashware for checking in the control unit or in the microprocessor of the control unit must be carried out in the way in which they were respectively carried out in the trust center in order to generate the transferred authentication code. A comparison of the hash value acquired by the microprocessor of the control unit with the transferred authentication code yields, if the two values correspond, in each case definitive information about the data integrity and authenticity of the transmitted flashware which has been buffered in the main memory. If both value correspond, the flashware is ~~respectively~~ considered to be error free.

[0056] After successful checking of the newly downloaded and buffered flashware, the flash boot loader writes the new buffered flashware into the flash memory of the control unit. The copying process from the main memory into the flash memory can additionally be checked here for completeness with a cyclic block protection method. If the authenticity checking and the copying process were error free, ~~what is referred to as~~ a flag is set for the flashware located in the flash, which ~~This flag~~ identifies the application program now located in the flash as the application program to be used as valid. As illustrated by way of example in figure 7, the flag can, for example be set here in the flash memory itself; ~~[[,]]~~ the flash memory is preferably embodied as an EEPROM. The control unit can then enter the application and in the process will use the application programs identified with a valid flag.

[0057] The flash boot loader is preferably actuated by the diagnostic system in a workshop. In this case, the diagnostic system of the workshop forms the system interface 4. In the case of the downloading process according to figure 1, unencrypted flashware and authentication code are buffered together into the main memory of the control unit by the system interface via the interface. In the case of the downloading process according to figure 2, the authentication code is buffered into the main memory of the control unit via the system interface, while the unencrypted flashware is buffered into the main memory of the control unit via a further reading device, preferably a CD-ROM disk drive or a chip card reading device. In the case of the downloading process according to figure 2, the reloading routine of the flash boot loader must therefore, if appropriate,

download the required data records from different electronic data processing systems. However, in all cases, communication in the vehicle takes place via the motor vehicle-internal data buses. A data bus which is widespread nowadays in motor vehicles ~~is what~~ is referred to as ~~[[the]]~~ a CAN bus.

[0058] Not all control units in a motor vehicle have sufficient memory space to be able to buffer the flashware. ~~In the case of~~ For control units in which the existing memory area is not sufficient to buffer the downloaded flashware, the downloading process is ~~therefore~~ carried out as follows:

- Firstly the existing flash memory is erased.
- The new flashware is then downloaded and programmed.
- The downloaded flashware is then verified, that is to say checked for transmission errors.
- The authentication checking is then carried out as in the preceding exemplary embodiments.
- After positive authenticity checking, the downloaded flashware is identified and actuated by setting a flag in the form of a status bit.
- the following applications then access the new flashware.

[0059] Directly downloading without buffering the flashware has the additional advantage of “end-to-end” protection since write errors are also detected in the writing process during the downloading process.

[0060] In all the exemplary embodiments of the invention, the flashware can have what is referred to as meta information added to it. This flashware meta information is, in particular, a vehicle identification number, a control unit parts number or a special memory location for the flashware. By including the flashware meta information it is possible, for example, to select the storage location for the flashware which is to be newly downloaded. Since the flashware meta information is also included in the calculation of the authentication code, this flashware meta information is also protected against manipulations.

[0061] The foregoing disclosure has been set forth merely to illustrate the invention and is not intended to be limiting. Since modifications of the disclosed embodiments incorporating the spirit and substance of the invention may occur to persons skilled in the art, the invention should be construed to include everything within the scope of the appended claims and equivalents thereof.

ABSTRACT OF THE DISCLOSURE

~~The invention relates to a~~ A simplified symmetrical, cryptographic method. ~~The basis of this method is based on an authentication code. This authentication code that~~ is calculated in a secured area, ~~referred to as~~ (a trust center) ~~[[,]]~~ by concatenating ~~[[the]]~~ an application program, ~~referred to as the flashware,~~ with a secret data string and calculating a hash value from the concatenated application program, and is checked in a . ~~This hash value is calculated here by means of the application program and by means of the secret data string. This hash value is the authentication code for the application program to be checked. The authentication code is checked in the microprocessor system or in the control unit in which the application program is to be used. For this purpose, a second, identical, secret data string is stored in the microprocessor system or the control unit. Firstly, After, the unencrypted application program and the authentication code are transmitted into the microprocessor system or into the control unit, the~~ [[. The]] unencrypted application program is ~~[[then]]~~ concatenated with the second, identical, secret data string in the ~~microprocessor system or in the control unit.~~ A hash value is then calculated by ~~this~~ using the concatenated application program, ~~in the microprocessor system or in the control unit.~~ If the calculated hash value and the transmitted authentication code correspond, the transmitted application program ~~or the transmitted flashware is considered to be authentic and is allowed to be~~ is stored in the flash memory and applied in the control unit, ~~or in the microprocessor system. In a development of the invention, the application program is~~

concatenated with the secret data string at both ends both at the start of the program and at the end of the program. The hash value is then calculated by means of the application program which is concatenated at both ends. In order to check the authentication code which is formed in this way, in the microprocessor system or in the control unit the application program which is transmitted in unencrypted form is also concatenated at both ends with the second, secret data string stored in the control unit, and a hash value is formed in the control unit or in the microprocessor system by means of the application program which is concatenated at both ends. If the hash value calculated in the control unit or in the microprocessor system corresponds to the transmitted authentication code, the transmitted application program is considered to be authentic. The concatenation at both ends has the advantage of improved protection against unacceptable manipulations of the application software.